

Serial No. 10/531,444
Atty. Docket No. P70537US0

REMARKS

The Office Action mailed October 16, 2008, has been carefully reviewed and, by this Amendment, Applicant has canceled claims 1-14, and added new claims 15-26. Claims 15-26 are pending in the application. Claims 15, 21 and 24 are independent.

The Examiner objected to the specification as containing informalities which Applicant has corrected herein including the addition of headings.

The Examiner objected to claims 1-14 as containing informalities. As set forth herein, claims 1-14 have been cancelled and new claims 15-26 added which are in conformity with U.S. practice. Favorable consideration of the new claims is requested.

The Examiner rejected claims 1-14 under 35 U.S.C. 101 as being directed to non-statutory subject matter. With the cancellation of claims 1-14, this rejection is technically moot. However, with respect to new claims 15-26, Applicant notes that the claimed invention is directed to a method using a transmitting device and a receiving device as set forth in claim 15, a system having transmitting and receiving components as set

Serial No. 10/531,444
Atty. Docket No. P70537US0

forth in claim 24, and a device having specified hardware components. Accordingly, new claims 15-26 are directed to statutory subject matter in accordance with 35 U.S.C. 101.

The Examiner rejected claims 1-14 as being anticipated by U.S. Publ. No. 2003/0069967 to Vincent. With the cancellation of claims 1-14, this rejection is technically moot. However, with respect to new claims 15-26, Applicant provides the following remarks.

As set forth in new claim 15, which is based upon original claim 1 and further includes the limitations of original claims 3 and 4, the present invention is directed to a method for security verification of a message (Msg) transmitted and received in electronic form. On the transmitting side, the message is associated with a univocal message identifier (ID_{Msg}) and a checking username (ID_{CR}) associated with the message owner for checking the identity of the message owner. At least the checking username (ID_{CR}) is assembled with the message and transmitted therewith, with this assembling taking place by inserting the message identifier (ID_{Msg}) into the message (Msg) and applying a coding operation previously associated with the message owner to the result of the insertion. On the receiving

Serial No. 10/531,444
Atty. Docket No. P70537US0

side for security verification of a received message (Msg), the message identifier (ID_{Msg}) of the received message is compared with previously received message identifiers to determine whether or not a message having the same univocal message identifier (ID_{Msg}) associated therewith has already been previously received. A decoding operation associated with a supposed owner of the received message is then applied to the checking username (ID_{CR}) of the owner associated with the received message to obtain an identifier (ID_{DCR}), and it is determined whether or not agreement exists between the univocal message identifier (ID_{Msg}) associated with the received message and the identifier (ID_{DCR}) obtained by the decoding operation performed on the checking username (ID_{CR}). This process is not shown by Vincent.

Vincent is directed to a system having a central computer that is able to authorize a client computer to make a limited number of accesses to data on a remote computer. To do so, Vincent teaches that the client computer sends a request to the central computer and the central computer provides the client computer with a response containing the authorization. The client computer sends this authorization to the remote computer which, in turn, sends to the client computer the information

Serial No. 10/531,444
Atty. Docket No. P70537US0

requested by the client computer. Should an unauthorized client computer intercept the response of the central computer, the unauthorized client computer might use it for accessing the information of the remote computer even if it does not have the right to do so.

The present invention, by contrast, has no authorizing entity (as in the central computer of Vincent). Rather, the client computer sends messages directly to a remote computer using a univocal message identifier and an associated encrypted copy thereof which allows for direct protection of messages being sent between a client computer and a remote computer.

In Vincent, on the other hand, the "nonce value" is generated and signed by the central computer. Vincent does not have a univocal identifier generated by the client computer and associated in encrypted form with the message sent by the client computer. Rather, in Vincent the central computer proceeds by digitally signing the nonce or the data request message, that are contained within the generated response, with a private encryption key that is associated with the operator of the central computer (see paragraph [0045]). A false nonce could be generated if the nonce is not signed and then a true signed

Serial No. 10/531,444
Atty. Docket No. P70537US0

message could be sent many times, or a signed nonce could be kept and the not-signed message be forged. Moreover, no precautions are taken in Vincent to prevent an ill-intentioned person from separating a signed nonce value from the response sent by the central computer to the client computer and producing therewith a false message to be sent to the remote computer.

In the present invention, the message identifier can be assembled with the message *before* encoding and the encoding can then be performed on the result of the assembly to have a checking username (ID_{CR}) incorporated in encrypted form in the transmitted message and then the result of the encoding is associated with the message identifier not encoded (see page 12, lines 9-14). In this way, it is impossible for an ill-intentioned person to separate the message from the identifiers in an effort to associate the identifiers with a false message.

The Examiner stated that original claims 3 and 4 were anticipated by Vincent. Reconsideration of this conclusion in view of new claim 15 is requested, however, as claim 15 provides that at least the checking username (ID_{CR}) is assembled with the message and transmitted therewith, and the assembling takes place by inserting the message identifier (ID_{Msg}) in the message (Msg)

Serial No. 10/531,444
Atty. Docket No. P70537US0

and applying the coding operation to the result of the insertion.

In Vincent, by contrast, the central computer proceeds to digitally sign the nonce or the data request message. The nonce is not inserted into the message and no coding operation is therefore applied to the result of the insertion. Further, in Vincent there is no teaching about the use of a complex message formed by a message identifier (ID_{Msg}) plus the result of the coding applied to the union of the message identifier (ID_{Msg}) and the message (Msg).

For at least the foregoing reasons, new claim 15 is patentable over Vincent. New independent claims 21 and 24 are also in condition for allowance for the same reasons as claim 15. Claims 16-20, 22, 23, 25 and 26 are also in condition for allowance as claims properly dependent on an allowable base claim and for the subject matter contained therein.


With this amendment and the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance.

Serial No. 10/531,444
Atty. Docket No. P70537US0

Should the Examiner have any questions or comments, the Examiner is cordially invited to telephone the undersigned attorney so that the present application can receive an early Notice of Allowance.

Respectfully submitted,

JACOBSON HOLMAN PLLC

By 
John C. Holman
Reg. No. 22,769

400 Seventh Street, N.W.
Washington, D.C. 20004-2201
Telephone: (202) 638-6666
Date: April 16, 2009
JCH:SCB
H:\2009\04-09\P70537US0 AMD.wpd